CLAIMS

WHAT IS CLAIMED IS:

1. A method of generating pseudo-random numbers using a linear feedback shift register in which the correlation between successive pseudo-random numbers is reduced, said method comprising sampling output sequences of said linear feedback shift register with a specified periodicity.

2. The method of Claim 1 wherein said linear feedback shift register generates said output sequences corresponding to maximal length sequences.

3. The method of Claim 1 wherein said specified periodicity is equal to the number of bits output by said linear feedback shift register.

4. The method of Claim 1 further comprising periodically switching between iterative outputs generated by two or more linear feedback shift registers.

5. The method of Claim 3 further comprising periodically switching between iterative outputs generated by two or more linear feedback shift registers.

6. The method of Claim 2 further comprising periodically switching between iterative outputs generated by two or more linear feedback shift registers.

7. A method of generating pseudo-random numbers using linear feedback shift registers in which the correlation between successive pseudo-random numbers is reduced, said method comprising periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register.

8. The method of Claim 7 wherein said linear feedback shift registers comprise linear shift registers capable of generating maximal length sequences.

9. The method of Claim 7 wherein said pseudo-random numbers are generated with period equal to the sum of each of the individual linear feedback shift register periods.

10. The method of Claim 8 wherein said pseudo-random numbers are generated with period equal to the sum of each of the individual linear feedback shift register periods.

11. A method of encrypting a pseudo-random number generated by a linear feedback shift register comprising operating a nonlinear operator on said pseudo-random number and one or more operands.

12. The method of Claim 11 wherein said nonlinear operator comprises an XOR function.

13. The method of Claim 12 wherein said one or more operands comprises one operand comprising a unique bit sequence corresponding to the LFSR currently used to generate said pseudo-random number.

14. The method of Claim 4 further comprising operating a nonlinear operator on said pseudo-random number and one or more operands.

15. The method of Claim 5 further comprising operating a nonlinear operator on said pseudo-random number and one or more operands.

16. The method of Claim 6 further comprising operating a nonlinear operator on said pseudo-random number and one or more operands.

17. A method of further encrypting a pseudo-random number generated from a linear feedback shift register by using a hashing function comprising:

receiving said pseudo-random number generated from said linear feedback shift register; and

varying the initial value of said hashing function over time by way of a function operating on one or more variables.

18. The method of Claim 7 further comprising:

receiving said pseudo-random number generated from said linear feedback shift register; and

varying the initial value of said hashing function over time by way of a function operating on one or more variables.

19. The method of Claim 18 wherein said one or more variables comprises the configuration of feedback taps associated with said linear feedback shift register.

20. The method of Claim 14 further comprising:

receiving said pseudo-random number generated from said linear feedback shift register; and

varying the initial value of said hashing function over time by way of a function operating on one or more variables.

21. The method of Claim 15 further comprising:

receiving said pseudo-random number generated from said linear feedback shift register; and

varying the initial value of said hashing function over time by way of a function operating on one or more variables.

22. The method of Claim 16 further comprising:

receiving said pseudo-random number generated from said linear feedback shift register; and

varying the initial value of said hashing function over time by way of a function operating on one or more variables.

23. An apparatus comprising digital hardware for generating pseudo-random numbers using a linear feedback shift register in which the correlation between successive pseudo-random numbers is reduced.

24. The apparatus of Claim 23 wherein said digital hardware comprises flip-flops and gates.